Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently amended): A digital signing method, comprising:

applying a secret key to a message to generate a digital signature for the message;

distributing ~~a digital signature attached message including~~ the generated digital signature and the message;

registering the generated digital signature and the message ~~digital signature attached message~~ as log data with a log list; and

providing said log list responsive to a request~~.~~,

wherein the action of applying a secret key includes applying the secret key to a data set comprising the message and computed data to generate the digital signature, the computed data being based on a previously generated digital signature and on a previous message that are retrieved from the log list,

wherein the action of distributing further includes distributing the computed data along with the generated digital signature and the message.

2. (Original): The digital signing method of claim 1, wherein said message is a hash value of another message.

3. (Canceled)

4. (Currently amended): The digital signing method of claim 1, wherein said log data further comprises a distribution destination, and wherein~~:~~

~~said registering log data of the digital signature attached message with a log list further comprises:~~

~~registering log data of a digital signature attached message with a log list,~~ said log data including a distribution destination attached thereto.

5. (Currently amended): The digital signing method of claim 1, said method further comprising:

permitting registration of the log data with said log list only when the data from a previously signed message ~~included in said digital-signature-attached message~~ is included in the latest log data registered with said log list.

6. (Original): The digital signing method of claim 1, further comprising:

obtaining a timestamp from a trusted authority, said timestamp generated by applying a second secret key to the digital signature, and a time; and

said distributing a digital-signature-attached message including the generated digital signature and the message, further comprises:

distributing a digital-signature-attached message including the generated digital signature, the timestamp, and the message.

7. (Currently amended): A digital signature verifying method, comprising:

accepting a digital-signature-attached message;

acquiring a log list of a digital signer, wherein said digital-signature-attached message may have been distributed by said digital signer is to be verified; and

checking whether log data of said digital-signature-attached message is registered in said log list, ~~and~~

if the log data is registered in the log list, authenticating that the digital-signature-attached message was distributed by the digital signer.; and

checking whether the digital signature included in the digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

8. (Canceled)

9. (Original): The digital signature verifying method of claim 7, wherein said digital-signature-attached message further comprises data from a previously signed message, said method further comprising:

checking whether the digital signature included in the digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature, the data from a previously signed message, and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

10. (Original): The digital signature verifying method of claim 9, said method further comprising:

checking whether data from a previously signed message included in said digital-signature-attached message is included in the log data registered immediately before log data of said digital-signature-attached message in said log list, and if the data from a previously signed message is included in the immediately previous registered log data, authenticating that said log list has not been altered.

11. (Original): The digital signature verifying method of claim 7, wherein said log data further comprises a distribution destination, said method further comprising:

acquiring a digital-signature-attached message from the distribution destination attached to the log data registered immediately before/after the log data of said digital-signature-attached message in said log list, and

checking whether the acquired message is included in said immediately previous/subsequent registered log data, and if the message is included, authenticating that said log list has not been altered.

12. (Original): The digital signature verifying method of claim 7, wherein said digital-signature-attached message further comprises a timestamp created using a second secret key, said method further comprising:

acquiring a digital signature and a time data by applying a public key paired with said second secret key to the timestamp included in said digital-signature-attached message; and

checking whether date and time indicated by the acquired time data exceeds a date and time of signing of said digital-signature-attached message, and if the date and time indicated by the time data does not exceed the date and time of signing of said digital-signature-attached message, authenticating the validity of the acquired digital signature.

13. (Currently amended): A digital signing apparatus, comprising:

a processor; and

a storage medium; wherein said processor applies a secret key to a message to generate a digital signature for the message; and wherein

~~said processor prepares a digital-signature-attached message including the generated digital signature and the message; and wherein~~

said processor registers log data ~~of said digital-signature-attached message~~comprising the digital signature and the message with a log list in said storage medium~~.~~; and wherein

said processor further applies the secret key to the message and to computed data to generate the digital signature, the computed data being determined based on a previously generated digital signature and on a previous message that are retrieved from the log list; and wherein

said processor distributes the computed data along with the generated digital signature and the message.

14. (Original): The digital signing apparatus of claim 13, wherein, said message is a hash value of another message.

15. (Canceled)

16. (Currently amended): The digital signing apparatus of claim 13, wherein said log data further comprises a distribution destination~~, and wherein:~~

~~said processor registers log data of a digital signature attached message with a log list, said log data including a distribution destination attached thereto~~.

17. (Currently amended): The digital signing apparatus of claim 13, wherein:

registration of the log data with said log list is permitted only when the data from a previously signed message ~~included in said digital signature attached message~~ is included in the latest log data registered with said log list.

18. (Currently amended): The digital signing apparatus of claim 13, wherein:

said processor obtains a timestamp from a trusted authority, said timestamp generated by applying a second secret key to the digital signature, and a time; and

said processor ~~prepares said digital signature attached message including the generated digital signature,~~further distributes the timestamp, along with the generated digital signature, the computed data, and the message.

19. (Original): The digital signing apparatus of claim 13, further comprising:

an interface configured to be connectable to a computer.

20. (Original): The digital signing apparatus of claim 19, wherein:

if a number of the log data registered with the log list exceeds a particular value, said processor outputs at least one of a plurality of log data registered with the log list to said computer, whereupon said computer registers said at least one of a plurality of log data with a second log list prepared in said computer, and thereupon,

said processor deletes said at least one of a plurality of log data from said log list in said storage medium.

21. (Currently amended): A digital signature verifying apparatus, comprising:

a processor interconnected with an input device, wherein:

said input device accepts a digital-signature-attached message to be verified and a log list of a digital signer; and wherein

said processor checks whether log data of said digital-signature-attached message is registered with said log list, and

if the log data is registered with the log list, authenticates that the digital-signature-attached message has been generated by said digital signer~~.~~,

wherein said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

22. (Canceled)

23. (Original): A digital signature verifying apparatus of claim 21, wherein said digital-signature-attached message further comprises data from a previously signed message, and wherein

said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature, the data from a previously signed message, and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer.

24. (Original): A digital signature verifying apparatus of claim 23, wherein

said processor checks whether the data from a previously signed message included in said digital-signature-attached message is included in the log data registered immediately before the log data of said digital-signature-attached message in said log list, and if

the data from a previously signed message is included in the immediately previous registered log data, said processor authenticates that said log list has not been altered.

25. (Original): The digital signature verifying apparatus of claim 21, wherein said log data further comprises a distribution destination, and wherein:

said processor acquires a digital-signature-attached message from the distribution destination attached to the log data registered immediately before/after the log data of said digital-signature-attached message in said log list, and wherein

said processor checks whether the acquired message is included in said immediately previous/subsequent registered log data, and if the message is included, said processor authenticates that said log list has not been altered.

26. (Original): The digital signature verifying apparatus of claim 21, wherein said digital-signature-attached message further comprises a timestamp created using a second secret key, and wherein:

said processor acquires a digital signature and a time data by applying a public key paired with said second secret key to the timestamp included in said digital-signature-attached message; and wherein

said processor checks whether date and time indicated by the acquired time data exceeds a date and time of signing of said digital-signature-attached message, and if the date and time indicated by the time data does not exceed the date and time of signing of said digital-signature-attached message, said processor authenticates the validity of the acquired digital signature.

27. (Currently amended): A computer program product for creating a digital signature, said program product comprising:

code that maintains a log list, the log list including messages and digital signatures;

code that applies a secret key to an original message and to computed data based on information retrieved from the log list comprising a previously generated digital signal and a previous message to generate a digital signature for the original message;

code that prepares a digital-signature-attached message including the computed data, the generated digital signature, and the original message;

code that registers log data of said digital-signature-attached message and the computed data with a log list in said storage medium; and

a computer readable storage medium for embodying the codes.

28. (Original): A computer program product of claim 27, wherein the computer readable storage medium is a computer readable medium for storing the codes.

29. (Original): A computer program product of claim 27, wherein the computer readable storage medium is a computer readable medium for transmitting the codes.

30. (Currently amended): A computer program product for verifying a digital signature, said computer program product comprising:

code that accepts a digital-signature-attached message and a log list from a digital signer; and

code that checks whether log data of said digital-signature-attached message is registered with said log list, and if the log data is registered with the log list, authenticates that the digital-signature-attached message has been generated by said digital signer, wherein said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the digital-signature-attached message,

using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer; and

a computer readable storage medium for storing the codes.

31 - 33. (Canceled)

34. (New): The digital signing method of claim 1 wherein the registering further includes registering the computed data.

35. (New): The digital signature verifying method of claim 7 wherein the digital-signature-attached message that is registered in the log list includes data based on a previously generated digital signature and on a previous message.

36. (New): The digital signing apparatus of claim 13 wherein said processor further registers the computed data.

37. (New): The digital signature verifying apparatus of claim 21 wherein the digital-signature-attached message that is registered in the log list includes data based on a previously generated digital signature and on a previous message.